THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	
Inventors:Matthew M. WILLIAMSON et al.	: Confirmation No. 2845
	:
U.S. Patent Application No. 10/687,694	: Group Art Unit: 2135
	:
Filed: October 20, 2003	: Examiner: Randal D. Moran
For: PROPAGATION OF VIRUSES THROUGH AN INFORMATION TECHNOLOGY NETWORK	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: BOARD OF PATENT APPEALS AND INTERFERENCES

BRIEF ON APPEAL

This brief is in furtherance of the Notice of Appeal, filed in this case on July 17, 2008.

The fees required under § 1.17(f) and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

TABLE OF CONTENTS

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P., a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S. H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

A. Total Number of Claims in Application

There are a total of 43 claims in the application, which are identified as claims 1-43.

B. Status of all the Claims

Claims 1-43 are pending.

Claims 1-43 are rejected.

Claims Canceled – None.

Claims withdrawn from consideration but not canceled – None.

Claims Allowed – None.

C. Claims on Appeal

Claims on appeal are claims 1-43.

IV. Status of Amendments

There are no outstanding un-entered amendments before the Examiner.

V. Summary of Claimed Subject Matter

The present invention relates generally to a method of monitoring propagation of viruses.

Claim 1

Independent claim 1 recites a method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host (See Instant specification in at least page 9, lines 1-8 and FIG. 5, element 500):

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host (See Instant specification in at least page 9, line 23, page 10, lines 25-28, page 11, lines 12-17, page 21, lines 19-23, page 23, lines 1-3 and FIG. 6, elements 612, 612, 614, and 616; FIG. 7, elements 704 and 712, FIG. 10, elements 1010, 1012, 1014, and 1016);

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record (See Instant specification in at least page 11, lines 6-15, and lines 28-31, page 12, lines 1-4, page 22, lines 23-28, page 22, line 31 through page 23, line 3, page 23, lines 21-23, and FIG. 7, element 708, FIG. 11, element 1104);

transmitting all requests to send data (See Instant specification in at least page 10, lines 9-12, page 14, lines 20-21);

storing in a buffer data relating to requests which identify a destination host not in the record (See Instant specification in at least page 12, lines 4-12 and lines 28-30,

page 13, lines 4-20, page 14, lines 8-29, page 23, lines 29-32, and FIG. 7, element 712, FIG. 11, element 1108).

Claim 29

Independent claim 29 recites a method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host:

over the course of a first time interval, monitoring creation of sockets within the first host to identify destination hosts identified therein (See Instant specification in at least page 6, line 14 through page 8, line 9, page 9, line 23, page 10, lines 25-28, page 11, lines 12-17, page 21, lines 19-23, page 23, lines 1-3 and FIG. 6, elements 612, 612, 614, and 616, FIG. 7, elements 704 and 712, FIG. 10, elements 1010, 1012, 1014, and 1016);

comparing identities of destination hosts monitored during the first time interval with destination host identities in a record (See Instant specification in at least page 11, lines 6-15, and lines 28-31, page 12, lines 1-4, page 22, lines 23-28, page 22, line 31 through page 23, line 3, page 23, lines 21-23, and FIG. 7, element 708, FIG. 11, element 1104); and

storing data from all sockets which identify monitored destination hosts not in the record (See Instant specification in at least page 12, lines 4-12 and lines 28-30, page 13, lines 4-20, page 14, lines 8-29, page 23, lines 29-32, and FIG. 7, element 712, FIG. 11, element 1108).

Claim 43

Independent claim 43 recites a method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host (See Instant specification in at least page 9, line 23, page 10, lines 25-28, page 11, lines 12-17, page 21, lines 19-23, page 23, lines 1-3 and FIG. 6, elements 612, 612, 614, and 616, FIG. 7, elements 704 and 712, FIG. 10, elements 1010, 1012, 1014, and 1016);

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record (See Instant specification in at least page 11, lines 6-15, and lines 28-31, page 12, lines 1-4, page 22, lines 23-28, page 22, line 31 through page 23, line 3, page 23, lines 21-23, and FIG. 7, element 708, FIG. 11, element 1104);

transmitting all requests to send data (See Instant specification in at least page 10, lines 9-12, page 14, lines 20-21); and

based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record (See Instant specification in at least page 12, lines 4-12 and lines 28-30, page 13, lines 4-20, page 14, lines 8-29, page 23, lines 29-32, and FIG. 7, element 712, FIG. 11, element 1108).

VI. Grounds of Rejection to be Reviewed on Appeal

A. The issue is whether claims 1-6, 8, 9, 14-18, 20, 21, 23, 29-35, 38, and 41-43 are unpatentable under 35 U.S.C 103(a) as being obvious over *Andersen* (U.S. Patent 6,122,740) in view of *Shipp* (GB Patent Application Publication 2 367 714).

B. The issue is whether claims 7 is unpatentable under 35 U.S.C 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Maher, III et al.* (US 7,058,974).

C. The issue is whether claims 10-13, and 24-27 are unpatentable under 35 U.S.C 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Ramanujan* (US 5,341,491).

D. The issue is whether claims 19 and 22 are unpatentable under 35 U.S.C 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Cunningham et al. (EP 0 986 229).*

E. The issue is whether claims 36-37, 39, and 40 are unpatentable under 35 U.S.C 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Andersen* (US 2002/0013858).

VII. Argument

A. Was the PTO correct in rejecting claims 1-6, 8, 9, 14-18, 20, 21, 23, 29-35, 38, and 41-43 under 35 U.S.C. 103(a) as being obvious over *Andersen* in view of *Shipp*?

Claim 1

The rejection of claims 1-6, 8, 9, 14-18, 20, 21, 23, 29-35, 38, and 41-43 as being obvious over *Andersen* in view of *Shipp* is hereby traversed.

Appellants first turn to the PTO's remarks found in the Advisory Action (AA) dated July 11, 2008.

First, the PTO asserts that Appellants argued "that *Shipp* does not appear to describe a record indicative of identifies of hosts within the network to whom data has been sent." AA at page 2, lines 3-4. Appellants do not appear to have argued this point in the After Final Amendment submitted June 17, 2008. Instead, as set forth below, Appellants pointed out that *Andersen*, as argued by the PTO, fails to disclose or suggest the claimed "establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host" as claimed in claim 1.

Furthermore, the distinction made by Appellants was that the PTO has referred to two different elements of *Andersen* (i.e., an access list and log data) to attempt to meet a feature (i.e., a record) claimed in the subject matter of claim 1. This is incorrect as set forth below and for at least this reason, reversal of the rejection is believed to be in order.

Second, the PTO asserts that "the combination [of *Andersen* and *Shipp*] discloses actions carried out by the first host." AA at page 2, lines 9-11. This is incorrect. With respect to *Andersen*, at least the establishing a record and storing in a buffer steps appear to be described as performed remotely. Further details are provided below with respect to the foregoing related to *Andersen*.

With respect to *Shipp*, the PTO asserts that "*Shipp* . . . discloses a logger as part of the system;" however, the PTO fails to identify that the "system" differs from the "system" relied on by the PTO with respect to *Andersen*. That is, in *Shipp* the "system" is a mail server and not a client system; whereas in *Andersen*, the "system" is the client system. Per *Shipp*, the logger 22 is a subsystem of an Internet service provider depicted in FIG. 2. See *Shipp* at page 5, lines 3-14 and FIG. 2. Thus, *Shipp* and *Andersen* refer to different systems and no reasoned rationale for combining the systems in the manner as asserted by the PTO has been set forth. Thus, the PTO has failed to identify that the actions are carried out by a first host as claimed. For at least this reason, reversal of the rejection is respectfully requested.

Further, the PTO asserts, without support in the reference, that *Andersen* discloses that "the access list . . . is made up of log data retrieved from the client device." This is incorrect. The PTO relied-on portion of *Andersen*, reproduced herein for convenience and ease of reference, states:

> Additionally, the identifier of the host system being accessed, for example the URL of the host system being accessed, may be extracted from the request and be included as the log data to be forwarded to log server 150 of FIG. 1, as discussed in more detail below. Additional log data may also be included by logging DLL 230, such as the date of the access, the time of the access, the

> elapsed time since the last host system was accessed, etc. Furthermore, according to one embodiment of the present invention, logging DLL 230 can provide site description information as part of the log data. For example, browser 210 may maintain a list of keywords or abstracts of certain sites being accessed by the individual user. If this list is maintained, then the keywords or abstract of the host system being accessed is included as part of the log data.
>
> Additionally, **logging DLL 230 is also coupled to a temporary access list 235**. Temporary access list 235 is a list of host systems which are not to be accessed by the user of the system. Alternatively, access list 235 may be a list of only those systems which can be accessed by the user. In the illustrated embodiment **access list 235 is obtained from log server 150** and is stored in volatile memory, such as the random access memory (RAM) of the system. The use of access list 235 by logging DLL 230 is discussed in more detail below. It should be noted that the data in **temporary access list 235 could also be encrypted** in any of a wide variety of conventional manners, and decrypted by logging DLL 230 whenever accessed.
>
> *Andersen* at column 5, lines 19-47 (emphasis added)

Based on the foregoing, *Andersen* appears to recite only that the logging DLL is coupled to a temporary access list which is obtained from the log server and may be encrypted. Conspicuously absent from the foregoing portion of *Andersen* is any description stating that the access list is "based on previous log data retrieved at the logging server." For at least this reason, reversal of the rejection is respectfully requested.

Third, addressing the PTO's assertions at lines 19-25 of page 2 of the AA, the PTO states that it would have been obvious to modify *Andersen* in view of *Shipp* "in order to identify patterns characteristic of a virus outbreak and take corrective action." This is incorrect for at least two reasons.

1. Assuming *arguendo* the combination of *Andersen* and *Shipp*, the PTO has failed to identify why a person of ordinary skill in the art at the time of the present invention would have combined the remote network access logging and reporting

functionality of *Andersen* with the email traffic monitoring system of *Shipp* as asserted by the PTO. The PTO has failed to identify how *Shipp*'s identification of patterns characteristic of a virus outbreak with respect to email is applicable to the remote network access logging of *Andersen*. For at least this reason, reversal of the rejection is respectfully requested.

2. Further, assuming *arguendo* the combination of *Andersen* and *Shipp*, the combination would appear to suggest the addition of an email monitoring system per *Shipp* as an additional virus monitoring capability to *Andersen* rather than suggesting a change in the remote network access logging operation of *Andersen* to operate in accordance with the *Shipp* system. The PTO has failed to identify a reason why a person of ordinary skill would selectively choose to incorporate the recited "storing in a buffer data relating to requests which identify a destination host" from *Shipp* into *Andersen*. The asserted motivation of being able to identify patterns characteristic of a virus outbreak and take corrective action appear unrelated to the asserted incorporated functionality. For at least this reason, reversal of the rejection is respectfully requested.

Fourth, addressing the PTO's assertions at lines 15-18 of page 2 of the AA, the PTO states that the "test is what the combined teachings of the references would have suggested to those of ordinary skill in the art." However, as set forth above in item 2. of the third set of remarks and as set forth below, the combination is still believed to be unsupported by the references for the following reasons: (1) *Andersen* already

includes storage space for storing data and (2) there is no blocking of network access requests in the relied-on FIG. 3 embodiment and therefore no reason to temporarily store "in a buffer data relating to requests which identify a destination host as taught by *Shipp*." Thus, the PTO has still failed to identify a motivation to combine the references without improperly relying on hindsight to reconstruct the present claimed subject matter. The PTO appears to be asserting that a person of ordinary skill in the art would add "storing in a buffer data relating to requests which identify a destination host" from *Shipp* in order to "identify patterns characteristic of a virus outbreak and take corrective action" in *Andersen*. The PTO has failed to provide support and/or articulated a reasoned rationale for this selective picking and choosing from *Shipp* to add a missing element to *Andersen*. For at least this reason, reversal of the rejection is respectfully requested.

Appellant turns now to the remainder of the arguments advanced in the Final Official Action (FOA) mailed April 17, 2008.

First, *Andersen* fails to disclose or suggest the claimed "establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host."

The PTO appears to assert that the access list of *Andersen* corresponds to the claimed feature; however, this is incorrect. *Andersen* fails to disclose that the access

list is indicative of hosts "to whom data has been sent by the first host" as claimed. The PTO has failed in both the FOA and the AA to identify any teaching in *Andersen* regarding how the access list entries are chosen. The PTO reference to column 5, lines 19-47 of *Andersen* is devoid of any teaching regarding access list entries comprising hosts to whom data has been sent by the first host. For at least this reason, reversal of the rejection is respectfully requested.

Second, claim 1 recites that the steps are "carried out by the first host" which the PTO has failed to identify in *Andersen*. Specifically, *Andersen* appears to recite that the steps, asserted by the PTO to correspond to the establishing and storing steps though not agreed to by Applicants, are performed remotely. That is, the establishment of the access list in *Andersen* is performed at the log server 150 by a supervisor, and the log data is stored at the log data store 520 of server 150.

Contrary to the PTO's assertions otherwise, notably at page 13, lines 10-14 of the Final Official Action (FOA), *Andersen* at column 10, lines 1-56 appears to state that the access list and log data should be maintained remotely from the client systems. The relevant portion of the relied-upon portion of *Andersen*, reproduced herein for ease of reference, states:

> In one embodiment, the method and apparatus for **remote** network access logging and reporting discussed above is implemented as a series of software routines run by a hardware system of FIG. 9. These software routines comprise a plurality or series of instructions to be executed by a processor in a hardware system, such as processor 902 of FIG. 9. Initially, the series of instructions are stored on a storage device, such as mass storage 920. The instructions are copied from storage device 920 into memory 914 and then accessed and executed by processor 902. . . .

It is also to be appreciated that the present invention can be used for the **remote logging** of any of a wide variety of activities which can be engaged in on a client system. For example, a client system 110 of FIG. 1 may be able to receive and display television programming. Thus, the television channel and time and date of viewing could be transferred to the log server as the log data. Additionally, channel description information could also be forwarded, such as selected text from the closed captioning information, or an electronic television guide which could be transferred during the vertical blanking interval, or data from a preview channel.

Thus, the present invention provides a method and apparatus for **remote network access logging and reporting**. A record of log data identifying at least the host systems accessed, as well as possibly additional information, **can be advantageously maintained at a remote location**. **The remote location can then be accessed by a supervisor at will, yet the data cannot be altered by an individual user because the data is stored remotely**. Furthermore, access to particular host systems can advantageously be prevented based on an access list which is obtained from a **remote** location at the time the present invention begins running. Thus, the access list is maintained remotely, thereby inhibiting an individual who may attempt to alter the list.

Andersen at column 10, lines 1-56 (emphasis added)

Based on the foregoing, *Andersen* appears to disclose remote maintenance of the access list and log data contrary to the recitation of claim 1. For at least this reason, reversal of the rejection is respectfully requested.

The PTO admits that *Andersen* does not disclose a method of monitoring propagation of viruses within a network of hosts comprises storing in a buffer data relating to requests which identify a destination host not in the record as claimed in claim 1. The PTO attempts to rely on *Shipp* to cure the deficiencies of *Andersen*. However, this is believed to be incorrect.

Third, *Andersen* already includes storage, i.e., log data store 520, for storing data about requests and the PTO has failed to identify why a person of ordinary skill in that art would have modified *Andersen* to include a temporary store as in *Shipp*. For at least this reason, reversal of the rejection is respectfully requested.

Fourth, in *Andersen* (as relied on by the PTO, specifically the non-blocking Fig. 3 embodiment of *Andersen*) there is no blocking and thus no need to temporarily store anything for later retrieval as asserted by the PTO. That is, the PTO has failed to identify a reason to include the temporary store of *Shipp* in *Andersen* because in the particular embodiment relied on by the PTO there is no storage of blocked emails needed in *Andersen*. As set forth above, the asserted rationale that a person of ordinary skill would combine the references in order to identify patterns characteristics of a virus outbreak and take corrective action is wholly unrelated to the temporary store and/or the addition thereof to *Andersen* and fails to provide a motivation for combining the references. For at least this reason, reversal of the rejection is respectfully requested.

Based on at least the foregoing, reversal of the rejection is respectfully requested.

Claims 2-6, 8, 9, 14-18, 20, 21, 23, and 42 depend, either directly or indirectly, from claim 1, include further features, and are patentable over *Andersen* in view of *Shipp* for at least the reasons advanced above with respect to claim 1.

The rejection of claims 2-82-6, 8, 9, 14-18, 20, 21, 23, and 42 should be reversed.

Claim 43 is patentable over *Andersen* in view of *Shipp* for at least reasons similar to those advanced above with respect to claim 1 and reversal of the rejection is respectfully requested.

Claim 29 is patentable over *Andersen* in view of *Shipp* for at least reasons similar to those advanced above with respect to claim 1 and reversal of the rejection is respectfully requested.

Claims 30-35, 38, and 41 depend, either directly or indirectly, from claim 29, include further features, and are patentable over *Andersen* in view of *Shipp* for at least the reasons advanced above with respect to claim 29. The rejection of claims 30-35, 38, and 41 should be reversed.

B. Was the PTO correct in rejecting claim 7 under 35 U.S.C. 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Maher, III et al.*?

Claim 7

The rejection of claim 7 under 35 U.S.C. 103(a) over *Andersen* in view of *Shipp* and further in view of *Maher, III et al.* (US 7,058,974) is traversed, *inter alia*, for at least the reasons advanced above with respect to claim 1. The rejection is respectfully requested to be reversed in view of the foregoing deficiencies of *Andersen* and *Shipp*.

C. Was the PTO correct in rejecting claim 10-13, and 24-27 under 35 U.S.C. 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Ramanujan*?

Claim 10-13, 24-27

The rejection of claims 10-13, 24-27 under 35 U.S.C. 103(a) over *Andersen* in view of *Shipp* and further in view of *Ramanujan* (US 5,341,491) is traversed, *inter alia*, for at least the reasons advanced above with respect to claim 1. The rejections are respectfully requested to be reversed in view of the foregoing deficiencies of *Andersen* and *Shipp*.

D. Was the PTO correct in rejecting claim 19 and 22 under 35 U.S.C. 103(a) as being obvious over *Andersen* in view of *Shipp* and further in view of *Cunningham*?

Claims 19 and 22

The rejection of claims 19 and 22 under 35 U.S.C. 103(a) over *Andersen* in view of *Shipp* and further in view of *Cunningham et al.* (EP 0 986 229) is traversed, *inter alia*, for at least the reasons advanced above with respect to claim 1. The rejections are respectfully requested to be reversed in view of the foregoing deficiencies of *Andersen* and *Shipp*.

E. Was the PTO correct in rejecting claim 36-37, 39, and 40 under 35 U.S.C. 103(a) as being obvious over *Andersen* in view of *Shipp and further in view of Andersen*?

Claims 36-37, 39, and 40

The rejection of claims 36-37, 39, and 40 under 35 U.S.C. 103(a) over *Andersen* is traversed, *inter alia*, for at least the reasons advanced above with respect to claim 1. The rejections are respectfully requested to be reversed in view of the foregoing deficiencies of *Andersen* and *Shipp*.

VIII. Conclusion

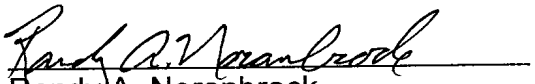
Each of the PTO's rejections has been traversed. Appellant respectfully submits that all claims on appeal are considered patentable over the applied art of record. Accordingly, reversal of the PTO's Final Rejection is believed appropriate and courteously solicited.

If for any reason this Appeal Brief is found to be incomplete, or if at any time it appears that a telephone conference with counsel would help advance prosecution, please telephone the undersigned, Appellant's attorney of record.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Reversal of the rejection is in order.

Respectfully submitted,
Matthew M. WILLIAMSON et al.

By: 
Randy A. Noranbrock
Registration No. 42,940
Telephone: 703-684-1111

HEWLETT-PACKARD COMPANY
IP Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80528-9599
Telephone: 970-898-7057
Facsimile: 281-926-7212
Date: **September 17, 2008**
RAN/bjs

IX. Claims Appendix

1. A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

automatically transmitting all requests to send data;

storing in a buffer data relating to requests which identify a destination host not in the record.

2. A method according to claim 1 wherein the record is established by monitoring identities of destination hosts to whom requests have been transmitted during a second time interval, which precedes the first time interval.

3. A method according to claim 2, wherein the record contains a predetermined maximum number of destination host identities, the maximum number being defined in accordance with a policy.

4. A method according to claim 3, wherein the policy additionally defines a maximum number of destination host identities not in the record, to whom requests may be legitimately transmitted in accordance with the policy.

5. A method according to claim 4 further comprising the step, at the end of any given time interval, of deleting from the buffer data relating to requests transmitted during the given time interval in accordance with the policy.

6. A method according to claim 5 further comprising the step, at the end of the given time interval, of updating the record to reflect identities of hosts identified in requests which are transmitted in accordance with the policy during the given time interval.

7. A method according to claim 6 further comprising the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with the policy.

8. A method according to claim 1, wherein the stored data is offered in the buffer and includes a copy of a socket created to send data in accordance with a request.

9. A method according to claim 8 wherein the socket enables identification of at least one application program at whose behest the socket is created.

10. A method according to claim 1 further comprising the steps of:

determining the value of parameter ("slack") based upon a number of successive time periods that pass when no new requests are made to send data from the first host to hosts not in the record; and

when slack exceeds a predetermined value, allowing un-impeded passage of data from the first host to destination hosts not in the record.

11. A method as claimed in claim 10, wherein slack is determined based upon the number of successive time periods for which the buffer is empty.

12. A method as claimed in claim 10, wherein slack has a predetermined maximum value.

13. A method as claimed in claim 10, wherein the value of slack is decremented each time an un-impeded passage of data from the first host to a destination host not in the record is allowed.

14. A method according to claim 10, wherein said time periods are of equal duration to at least one of said time intervals.

15. A method according to claim 1 further comprising the steps of

monitoring the rate of increase in the size of the buffer, and

in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a virus warning.

16. A method according to claim 1 further comprising the steps of

monitoring the increase in the size of the buffer per time interval, and

in the event that the increase in the size of the buffer in any given time interval exceeds a predetermined size, generating a virus warning.

17. A method according to claim 1 further comprising the steps of

monitoring the size of the buffer, and

in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a virus warning.

18. A method as claimed in claim 1, further comprising the step of varying with time at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record.

19. A method as claimed in claim 18, wherein said at least one parameter is varied as a function of the time of day.

20. A method as claimed in claim 18, wherein said at least one parameter is varied in response to a perceived threat level.

21. A method as claimed in claim 18, wherein said at least one parameter is changed between a first set of values and a second set of values at a predetermined rate.

22. A method as claimed in claim 21, wherein at least one of the values of said at least one parameter is randomly changed according to a predetermined probability distribution as a function of time.

23. A method as claimed in claim 1, further comprising the step of determining at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record by performing an automated search on a set of data indicative of normal network traffic.

24. A method according to claim 1 further comprising the steps of:

receiving a request to send a multiple recipient email from the first host;

determining the value of a parameter ("mslack") based upon the number of successive time periods that pass when no multiple recipient emails are sent from the first host;

if mslack exceeds a predetermined value, allowing un-impeded passage of the multiple recipient email.

25. A method according to claim 24, wherein the multiple recipient email is allowed un-impeded passage if mslack is greater than or equal to the number of intended recipients of the email.

26. A method as claimed in claim 24, wherein mslack is set to zero after the multiple recipient email has been sent.

27. A method as claimed in claim 24, wherein mslack has a predetermined maximum value.

28. A method according to claim 24, wherein said time periods are of equal duration to at least one of one or more time intervals.

29. A method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host:

over the course of a first time interval, monitoring creation of sockets within the first host to identify destination hosts identified therein;

comparing identities of destination hosts monitored during the first time interval with destination host identities in a record; and

storing data from all sockets which identify monitored destination hosts not in the record.

30. A method according to claim 29 wherein the stored socket data at least enables identification of the destination host identified therein.

31. A method according to claim 29 wherein the record identifies a maximum number of destination hosts, the maximum number being determined in accordance with a policy.

32. A method according to claim 31 wherein the record is established by monitoring creation of sockets during a time interval preceding the first time interval.

33. A method according to claim 31 wherein the policy additionally specifies a maximum number of sockets, each identifying a destination host not in the record, to be legitimately created in any given time interval.

34. A method according to claim 33 wherein at the end of a time interval, socket data containing identities of destination hosts in respect of whom sockets have legitimately been created is deleted.

35. A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host.

36. A method according to claim 35 wherein packets having a designated destination IP address are stored.

37. A method according to claim 36 further comprising the step of establishing the predetermined IP address from the stored socket data.

38. A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing incoming packets to the first host.

39. A method according to claim 38 wherein packets having a designated source IP address are stored.

40. A method according to claim 39, further comprising the step of establishing the predetermined IP address from the stored socket data.

41. A method according to claim 29 wherein socket data is stored in a buffer.

42. A method according to claim 1, wherein the step of automatically transmitting all requests comprises transmitting the data related to the requests.

43. A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

automatically transmitting all requests to send data regardless of a result of said comparing; and

based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record.

X. Evidence Appendix

None.